UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/712,237	11/13/2003	Joseph Wayne Freeman	RPS920030150US1 (111)	8584

50594 7590 09/30/2008

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2132	

MAIL DATE	DELIVERY MODE
09/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/712,237	FREEMAN ET AL.	
	Examiner	Art Unit	
	Venkat Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 4-7* is/are rejected.

7)☒ Claim(s) *2-3* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 7/21/2008 have been fully considered but they are not persuasive with respect to Claim 1.

Applicant argues that the reference fails to disclose reducing boot time of a Trusted Computing Performance Alliance(TCPA) based computing system and executing the boot code comprising a Core Root of Trust for Measurement(CRTM).

The Examiner contends that the Trusted Computing Performance Alliance based computing system is disclosed in Nguyen. Nguyen discloses standardization of computing platforms used and mentions the GUIDs defined by the manufacturers before shipment see Par. 0030. And furtherdiscloses verifying the BIOS image being conformed to industry standards see Par. 0031. The standardization and compliance with the norms of industry is akin to the Trusted Computing Performance Alliance specifications where the standardization are followed as disclosed by the specifications see Page 1 Ln 22- Page 2 Ln 2.

The reducing of boot time is also disclosed by Nguyen. Nguyen discloses the loading of BIOS image and this loading taking place in a flash part of memory as opposed to ROM in order for processing to take fast see Par. 0028. And further discloses the secondary portion and primary portion and the updated BIOS being loaded into the secondary portion see Par. 0036. This secondary portion is being loaded to memory first for execution and hence getting processed first see Par. 0040.

The Applicant also argues that reading bits in a register and indication of segments have been updated are not disclosed by Nguyen. Nguyen discloses the notification bit being used to indicate the updating of Nguyen see Par. 0026. And verifying of integrity of data see Par. 0033.

The Applicant's argument with regard to Claim 2 is persuasive.

Claim Rejections - 35 USC § 103

1. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 2004/0193865 to Nguyen et al.(hereinafter Nguyen) in view of US Patent 6581159 to Nevis et al.(hereinafter Nevis).

Regarding Claim 1, Nguyen discloses resetting said TCPA computing system see Par. 0026; executing a boot block code comprising a Core Root of Trust for Measurement (CRTM) see Par. 0017; reading bits in a register of a flash memory storing said boot block code, wherein said bits in said register indicate whether segments of said flash memory have been updated see Par. 0022; But does not explicitly disclose the hash values being used. However, Nevis discloses the obtaining one or more measurement values from a table storing hashed values from a previous measurement of a Power On Self Test (POST) Basic Input/Output System (BIOS) if one or more of said bits read in said register indicate one or more of said segments of said flash memory storing said POST BIOS have not been updated see Col 5 Ln 15-25. It would be obvious to one having ordinary skill in the art at the time of the invention to include hash values in the

invention of Nguyen in order to verify/unlock the hardware as taught in Nevis see Col 5 Ln 21-24.

Regarding Claim 4-5, Nguyen discloses the comparing of values and taking appropriate action if the values do not match see Fig. 3 item 316& 314 & Par. 0031.

Regarding Claim 6-7, Nguyen discloses the resetting of value and transmitting value to memory that the notify that it has been updated see Fig. 3 item 310 & 316 & 322.

Allowable Subject Matter

Claims 2-3 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is (571)272-7213. The examiner can normally be reached on 8:30-5:00. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. P./
Examiner, Art Unit 2132
September 26, 2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132